EXHIBIT A

UNITED STATES DISTRICT COURT

for the

Northern District of California

In re Application of Centripetal Networks, LLC,

Plaintiff

v.

Defendant

Civil Action No.

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To: Cisco Systems, Inc.
170 West Tasman Drive, San Jose, CA 95143

(Name of person to whom this subpoena is directed)

☑ *Production:* **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material: SEE SCHEDULE A

Place:	Date and Time:

☐ *Inspection of Premises:* **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: _____

CLERK OF COURT

OR /s/ Kristopher Kastens

Signature of Clerk or Deputy Clerk *Attorney's signature*

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* Centripetal Networks, LLC, , who issues or requests this subpoena, are: Kristopher B. Kastens, 333 Twin Dolphin Dr., Suite 700, Redwood Shores, CA 94065, (650) 752-1700, kkastens@kramerlevin.com

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____

on *(date)* _____ .

❒ I served the subpoena by delivering a copy to the named person as follows: _____

_____

_____ on *(date)* _____ ; or

❒ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

SCHEDULE A

1. Unless otherwise specified, the terms used in these Document Requests shall have the following meanings, and responses to these Requests shall be provided in accordance with the following instructions:

DEFINITIONS

2. These Requests hereby incorporate the definitions and instructions set forth in Rule 45 of the Federal Rules of Civil Procedure and the Local Rules for the United States District Court for the Northern District of California, except as modified herein. These Requests and the terms used herein shall be construed to require the fullest disclosure by law.

3. "Cisco," "You," or "Your" refer to Cisco Systems, Inc.

4. "Centripetal" refers to Centripetal Networks, LLC

5. "Source Code" means human-readable programming language text that defines software, firmware, or electronic hardware descriptions. Source Code files include without limitation files containing code in "C," "C++," "C/C++ Header," "Ruby," "Go," "SQL," "Python," "Java," "JavaScript," "ERB," "Objective C," "Objective C++," "Clojure," "Perl," and assembler, VHDL, and Verilog programming languages. Source Code files further include without limitation "include files," "make" files, link files, and other human-readable text files used in the generation and/or building of software and/or hardware.

6. "Accused Switch" or "Accused Switches" means Cisco's Catalyst 9300, 9400, and 9500 series that run on the software IOS-XE 16.5 and subsequent releases, and Catalyst 9800 series wireless controllers that run on the software IOS-XE 16.10 and subsequent releases.

7. "Accused Router" or "Accused Routers" means Cisco's Aggregation Services Router ("ASR") 1000 series and Integration Services Router ("ISR") 1000 and 4000 series which run on the software IOS-XE 16.5 and subsequent releases.

8. "Accused Firewall" or "Accused Firewalls" means Cisco's NextGeneration firewalls, specifically Cisco's Adaptive Security Appliance ("ASA") 5500 series with Firepower services that run ASA software version 9.4 and subsequent releases, and Cisco's Firepower Appliance 1000, 2100, 4100, and 9330 series that run Firepower Threat Defense software version 6.0 and subsequent releases.

9. "TCAM" means ternary content-addressable memory.

10. "Document" means, without limitation, all writings and records, including originals and all copies, unless identical, regardless of origin or location, of written, recorded, and graphic matter, however produced or reproduced, formal or informal, including any form of communication, correspondence, memoranda, letters, facsimiles, e-mails, text messages, instant messages, drafts, reports, financial statements, notes (including stenographic notes), records, envelopes, telegrams, telephone logs, messages (including reports, notes, and memoranda of personal or other telephone conversations and conferences), contracts, agreements, summaries, photographs, phonograph, tape or other records, disks, data cells, drums, printouts, and other compilations from which information can be obtained (translated, if necessary, through detection devices into usable form) and any other writings or documents of whatever description or kind including attachments or other matters affixed thereto and copies of any of the foregoing in your possession, custody, or control, including any material described above that originally may have been generated by any party hereto and is now in your possession, custody, or control. "Document" shall also include all drafts of documents defined above. A non-identical copy is a separate document within the meaning of this term. "Request" means a document request stated herein.

INSTRUCTIONS

1. In responding to these Requests, You shall produce all responsive Source Code, which is in Your possession, custody, or control, or in the possession, custody, or control of Your predecessors, successors, parents, subsidiaries, divisions, or affiliates, or any of Your respective directors, officers, managing agents, agents, employees, attorneys, accountants, or other representatives. Source Code shall be deemed to be within Your control if you have the right to secure the Source Code or a copy of the Source Code from another person having possession or custody of the Source Code.

2. The method through which You shall produce Source Code in Response to these Requests shall be done in strict accordance with the Protective Order in the Action.

3. The following rules of construction shall apply to these Requests:

(a) The terms "all" and "any," whenever used separately, shall be construed as "any and all" to encompass the greatest amount of responsive material.

(b) The connectives "and" and "or" shall be construed either disjunctively or conjunctively as necessary to bring within the scope of the request all responses that might otherwise be construed to be outside of its scope.

(c) The term "including" shall be construed to mean "including, but not limited to," or "including, without limitation" to encompass more than the specifically identified materials.

(d) The use of the singular form of any word includes the plural and vice versa.

4. You are requested to produce the requested Source Code in its entirety. If any portion of Source Code that is responsive cannot be produced, the remainder of the Source Code should be produced to the fullest extent possible with an explanation as to why production of the excluded portion is not possible.

5. If requested Source Code is no longer in Your possession, custody, or control, identify the Source Code and state what disposition was made of it and the date or dates upon which such disposition was made, and additionally, produce all Documents relating to the disposition of such Source Code.

6. If You object to any Request or portion thereof, state the reason or the objection in detail and respond to that Request as narrowed by Your objection.

7. If any of the requested Source Code is withheld in whole or in part under any claim of privilege, work product, or other immunity, then consistent with applicable law, You are to provide a list identifying the Source Code, for which any such privilege, work product, or other immunity is claimed, together with the following information:

(a) the nature of the claim of privilege or immunity;

(b) the pertinent facts relied upon in support of the claim of privilege or immunity;

(c) all persons on whose behalf the privilege or immunity is claimed;

(d) the subject matter (without revealing the information as to which privilege is claimed); and

(e) the date the Source Code was created.

You are further directed to describe the factual and legal basis for each claim of privilege or immunity in sufficient detail so as to permit the court to adjudicate the validity of the claim of privilege or immunity.

8. If there is no Source Code responsive to any particular Request, you shall so state in writing.

9. Each Request is continuing in nature. If any Source Code responsive to a Request is not presently in your possession, custody, or control but subsequently becomes available, is

discovered, is created, or comes into your possession, custody, or control, You are hereby requested to supplement Your responses to the Request within a reasonable period of time thereafter.

REQUESTS

1. Source Code relating to the feature(s) in Cisco's Accused Switches, Accused Routers, and Accused Firewalls that cause the product to stop processing packets under an old rule set and begin processing packets under a new rule set.

2. Source Code relating to the feature(s) in Cisco's Accused Switches, Accused Routers, and Accused Firewalls that cause the product to cease processing packets and to cache packets during a switch in rule sets.

3. Source Code relating to the feature(s) in Cisco's Accused Switches, Accused Routers, and Accused Firewalls that cause the product to resume processing packets after a switch to a new rule set.

4. Source Code relating to the technology described in Cisco's Hitless ACL specification attached as Exhibit A-1.[1]

5. Source Code relating to the Hitless ACL feature(s) in Cisco's Accused Switches and Accused Routers that return a "success" output after adding new rules to the TCAM and deleting old rules from the TCAM.

6. Source Code relating to the feature(s) in Cisco's Accused Switches and Accused Routers that cause the product to complete a reconfiguration process, including to move a new rule set into the TCAM, validate that the move occurred, and validate the completion of the process.

7. Source Code implementing Hitless ACL Change Flow steps 7 through 11 in Cisco's Accused Switches and Accused Routers.

[1] Exhibit A-1 is an excerpt from Plaintiff's Trial Exhibit PTX-1195, in Case No. 18-cv-00094-HCM, and was previously publicly disclosed.

8. Source Code relating to the technology described in Cisco's configuration guide describing the transactional commit model attached as Exhibit A-2.[2]

9. Source Code relating to the transactional commit model in Cisco's Accused Firewalls that cause the product to compile new rules and then verify that compilation of new rules is complete.

10. Source Code relating to the transactional commit model in Cisco's Accused Firewalls that cause the product to switch from processing packets using old rules to processing packets using new rules that are compiled and ready for use.

[2] Exhibit A-2 is an excerpt from Plaintiff's Trial Exhibit PTX-1293, in Case No. 18-cv-00094-HC, and was previously publicly disclosed.

EXHIBIT A-1

Document Number	EDCS-11690559
Based on Template	EDCS-189230 Rev 26
Created By	Joanne Maruca

FED 2.0 Hitless ACL Update Software Functional Specification

Add support for Hitless (Atomic) ACL update feature.

<<ISO requirement>>

N/A

Reviewers

Department	Name/Title
Development Engineering	Luh-Luh Ting, Caina Wei, Stanley Phung, Na Li, Wanzhen Yu
Development Test / QA Engineering	Allen Chen, Nirupa Gnanasekaran, Saravan Asthi

Modification History

Revision	Date	Originator	Comments
1	July 3, 2017	Joanne Maruca	Template to generate document number
2	July 9, 2017	Joanne Maruca	Initial version
3	July 12, 2017	Joanne Maruca	Address review comments

Plaintiff's Trial Exhibit
PTX-1195
Case No. 18-cv-00094-HCM

Table of Contents

1 Problem Definition

When an ACL is attached to an interface and then the ACEs in the ACL are changed, packets are being dropped.

<<ISO requirement>>

N/A

2 Software Architecture

An ACL change event is when an ACE is added, removed, modified or re-sequenced for the ACL. When an ACL change happens an event is sent to FMAN-RP, then to FMAN-FP, the ACL in CGD is updated and a new event is sent to FED for programming.

2.1 Current ACL Change Flow

Currently whenever there is a change to the ACE in an ACL, the data will drop packets during the change to hardware programming.

This is the sequence of events today:

1. ACE added, removed, modified or re-sequenced
2. An ACL Class Group (CG) change event is sent to FED
3. FED CFM is updated with new Policy CG information
4. All features using this Policy CG are updated
   a. Create new Policy to use temporarily
   b. Generate a new VMR list
   c. Merge and Optimize new VMR list
   d. Write the Drop Policy label to every LE attached to the old Policy
   e. Remove existing TCAM entries
   f. Overwrite old Policy with new Policy in SDK
   g. Delete new Policy
   h. Write new TCAM entries
   i. Validate which will write the Policy label back into all LE attached to Policy
   j. Return SUCCESS

On ERROR returned from writing entries into TCAM:

- If TCAM is full then leave with Drop Policy label programmed (UNLOADED)
- Display UNLOADED or ERROR message to console to indicate hardware was not programmed with new Policy
- Drop all packets for this protocol type, in this direction on the interface
- Return ERROR

2.2 Hitless (Atomic) ACL Change Flow

For this new feature Hitless (Atomic) ACL Change, no packets should drop while programming the new TCAM entries. To allow this to happen a new policy will be created and attached to the interface before deleting the existing policy.

This will always be enabled for all features that set the flag acknowledging support for hitless acl change; and is only available to features that go through ACL common code.

This is the new sequence of events:

1. ACE added, removed, modified or re-sequenced
2. An ACL Class Group (CG) change event is sent to FED
3. FED CFM is updated with new Policy CG information
4. All features using this Policy CG are updated
5. Generate a new VMR list
6. Merge and Optimize new VMR list
7. Verify if feature supports hitless ACL change
   - If supported, continue to Step 8
   - If not, use old method starting at Section 2.1 step 4d
8. Add new VCUs into hardware
9. Add new TCAM entries
10. Delete old entries from TCAM
11. Return SUCCESS

On ERROR returned from either of the new steps 7 or 8 will cause it to go back to use the old method of programming described in Section 2.1 starting with step 4d. So then, it will no longer be hitless.

<<ISO requirement>>

N/A

3 Software Requirements

The label will not be changed on the Policy. Just as the current Hitless QoS feature does, the new entries will be added with the existing label and there will be a short period where both sets of VMR entries will be installed before the old entries are deleted.

This will only be supported for these ACL features:

PACL, RACL, VACL, CGACL, and SGACL

This is targeted for software release 16.8.1

<<ISO requirement>>

N/A

4 Memory and Performance Impact

ACL change requests for large ACLs and/or attached to many interfaces may take longer to program in hardware with this feature.

<<ISO requirement>>

N/A

5 Packaging Considerations

N/A

<<ISO requirement>>

N/A

6 End User Interface/User Experience

Feature will always be enabled, no CLI changes.

With ACL change requests for large ACLs it may take longer to program in hardware with this feature if there is not enough room in TCAM to add the entries first and it has to revert to the old method.

<<ISO requirement>>

N/A

7 Configuration and Restrictions

Feature is enabled by default.

On ERROR conditions (no labels or out of TCAM space) it will fall back to the previous change method of deleting the old ACL and then installing the new ACL.

If with old method, there is still an ERROR programing, the ACL will be UNLOADED or an ERROR message will display on the console depending on the feature specific action.

<<ISO requirement>>

N/A

8 Testing Considerations

These are the recommended tests to verify this feature's functionality.

Each feature needs to be tested individually that will support the Hitless ACL Change feature, these are: **PACL, RACL, VACL, CGACL (wired clients only), and SGACL**

These tests all require traffic to be flowing to verify hitless change is happening. It will be required to have a set of streams per interface that has the ACL attached. Streams to show untouched permit and deny ACEs did not change and another one to show touched permit and deny ACEs did change. Need to test for all ACL types IPv4, IPv6, and MAC.

Testing should be done on Nyquist (Fiber and Copper), Edison, and Macallan platforms.

8.1 Basic Testing

Add an ACL to the interface for feature under test then do these tests to verify hitless change.

8.1.1 Modify existing ACE

8.1.2 Delete an existing ACE

8.1.3 Add a new ACE

8.1.4 Re-sequence the ACEs

8.2 Multiple Interface Testing

Attach ACL to multiple interfaces for the feature type under test and verify hitless change. Include interfaces on the same ASIC but different cores (for Doppler D platforms).

8.2.1 Modify existing ACE

8.2.2 Delete an existing ACE

8.2.3 Add a new ACE

8.3 Multiple ACL Testing

Perform tests with the same ACL on multiple interfaces and a different one on other interfaces. Do the following and verify that no traffic is impacted for the unchanged ACL and the changed ACL has the correct behavior.

8.3.1 Modify existing ACE

8.3.2 Delete an existing ACE

8.3.3 Add a new ACE

8.4 Multiple Feature Testing

Attach the same ACL to multiple feature interfaces test and verify hitless change for all. Include interfaces on the same ASIC but different cores (for Doppler D platforms); interfaces on the same ASIC; and interfaces on different ASICs.

The multiple feature sets should include at a minimum the following feature combinations.

8.4.1 PACL and RACL

8.4.1.1 Modify existing ACE

8.4.1.2 Delete an ACE

8.4.1.3 Add a new ACE

8.4.2 RACL and VACL (vlmap)

8.4.2.1 Modify existing ACE

8.4.2.2 Delete an ACE

8.4.2.3 Add a new ACE

8.4.3 SGACL and RACL

8.4.3.1 Modify existing ACE

8.4.3.2 Delete an ACE

8.4.3.3 Add a new ACE

8.5 Scale Testing

8.5.1 PACL

Add ACL that will consume just less than half of the available TCAM entries for the switch that is being tested. Verify all changes are hitless.

8.5.1.1 Modify existing ACE

8.5.1.2 Delete an ACE

8.5.1.3 Add a new ACE

8.5.2 VACL – Negative Test, not hitless, with UNLOADED message

Add ACL that will consume more than half of the available TCAM entries for the switch that is being tested. There will not be enough TCAM space and it will be forced to the old method of programming.

8.5.2.1 Modify existing ACE

8.5.2.2 Delete an ACE

8.5.2.3 Add a new ACE

8.5.3 RACL – Negative Test, not hitless, with UNLOADED message

Add ACL that will consume 5 VCU bits for the switch that is being tested. When try to add the VCU entries it will fail and will be forced to the old method of programming.

8.5.3.1 Add a new ACE to consume 2 more VCU bits

<<ISO requirement>>

N/A

9 Initiative, Legal, & Regulatory

<CPDM requirement>

N/A

10 Attachments

As appropriate, attach log sheets, diagrams, schematics, usability research, examples of forms, or other pieces of information used in or generated in the production of the document.

10.1 Review Action Items

1. Identify which release is targeted.
2. Update Section 8 for testing to include which platforms, ASIC/ASIC instances for interface to use, and protocol types to test.
3. Add test cases for multiple ACLS and VCU exhaustion.

<<ISO requirement>>

N/A

End of Document

EXHIBIT A-2

CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.8

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Plaintiff's Trial Exhibit
PTX-1293
Case No. 18-cv-00094-HCM

You must enable hardware bypass without the **sticky** option for the boot delay to operate. Without the **hardware-bypass boot-delay** command, the hardware bypass is likely to become inactive before the ASA FirePOWER module finishes booting up. This scenario can cause traffic to be dropped if you configured the module to fail-close, for example.

Step 4 Disable TCP sequence randomization. This example shows how to disable randomization for all traffic by adding the setting to the default configuration.

policy-map global_policy

class sfrclass

set connection random-sequence-number disable

If you later decide to turn it back on, replace "disable" with **enable**.

Step 5 Establish dual power supplies as the expected configuration:

power-supply dual

Adjust ASP (Accelerated Security Path) Performance and Behavior

The ASP is an implementation layer that puts your policies and configurations into action. It is not of direct interest except during troubleshooting with the Cisco Technical Assistance Center. However, there are a few behaviors related to performance and reliability that you can adjust.

Choose a Rule Engine Transactional Commit Model

By default, when you change a rule-based policy (such as access rules), the changes become effective immediately. However, this immediacy comes with a slight cost in performance. The performance cost is more noticeable for very large rule lists in a high connections-per-second environment, for example, when you change a policy with 25,000 rules while the ASA is handling 18,000 connections per second.

The performance is affected because the rule engine compiles rules to enable faster rule lookup. By default, the system also searches uncompiled rules when evaluating a connection attempt so that new rules can be applied; because the rules are not compiled, the search takes longer.

You can change this behavior so that the rule engine uses a transactional model when implementing rule changes, continuing to use the old rules until the new rules are compiled and ready for use. With the transactional model, performance should not drop during the rule compilation. The following table clarifies the behavioral difference.

Model	Before Compilation	During Compilation	After Compilation
Default	Matches old rules.	Match new rules. (The rate for connections per second decreases.)	Matches new rules.

Model	Before Compilation	During Compilation	After Compilation
Transactional	Matches old rules.	Match old rules. (The rate for connections per second is unaffected.)	Matches new rules.

An additional benefit of the transactional model is that, when replacing an ACL on an interface, there is no gap between deleting the old ACL and applying the new one. This feature reduces the chances that acceptable connections may be dropped during the operation.

Tip If you enable the transactional model for a rule type, syslogs to mark the beginning and the end of the compilation are generated. These syslogs are numbered 780001 through 780004.

Use the following procedure to enable the transactional commit model for the rule engine.

Procedure

Enable the transactional commit model for the rule engine:

asp rule-engine transactional-commit *option*

Where the options are:

- **access-group**—Access rules applied globally or to interfaces.
- **nat**—Network Address Translation rules.

Example:

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

Enable ASP Load Balancing

The ASP load balancing mechanism helps avoid the following issues:

- Overruns caused by sporadic traffic spikes on flows
- Overruns caused by bulk flows oversubscribing specific interface receive rings
- Overruns caused by relatively heavily overloaded interface receive rings, in which a single core cannot sustain the load.

ASP load balancing allows multiple cores to work simultaneously on packets that were received from a single interface receive ring. If the system drops packets, and the **show cpu** command output is far less than 100%, then this feature may help your throughput if the packets belong to many unrelated connections.